UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
FORT WAYNE DIVISION

ANTHONY WEBSTER and MARK SMITH, on behalf of themselves, and all others similarly situated,	)	
Plaintiffs,	)	
v.	)	CASE NO.: 1:24-CV-00117-HAB-SLC
BRADFORD-SCOTT DATA, LLC, doing Business as SHARETEC	)	
Defendant,	)	

OPINION AND ORDER

Plaintiffs Anthony Webster and Mark Smith, on behalf of themselves and all other similarly situated (collectively hereafter "Plaintiffs"), sued Defendant, Bradford-Scott Data LLC ("Bradford-Scott"), because hackers infiltrated Bradford-Scott's network and stole Plaintiffs' personal information. (ECF No. 29). Plaintiffs allege that Bradford-Scott failed to implement reasonable measures to safeguard their information and failed to promptly notify Plaintiffs of the data breach. Plaintiffs' suit asserts claims for negligence, negligence per se, breach of implied contract, invasion of privacy, unjust enrichment, and breach of bailment. Before the Court is Bradford-Scott's Motion to Dismiss Plaintiffs' Amended Complaint (ECF No. 25) in its entirety. In the alternative, it asks the Court to strike several paragraphs of Plaintiffs' Amended Complaint which it believes are immaterial. (*Id.*). Bradford-Scott's Motion is now fully briefed (ECF Nos. 25, 29, 31) and ripe for ruling.

I. Standard or Review

Defendant moves under Fed. R. Civ. P. 12(b)(6) which provides for the dismissal of a

complaint, or any portion of a complaint, for failure to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citations and internal quotation marks omitted); *see also Ray v. City of Chi.*, 629 F.3d 660, 662-63 (7th Cir. 2011). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*. When analyzing a motion to dismiss a claim under Rule 12(b)(6), the factual allegations in the complaint must be accepted as true and viewed in the light most favorable to the plaintiff. *Brokaw v. Mercer Cnty.*, 235 F.3d 1000, 1006 (7th Cir. 2000). That said, the Court is not "obliged to accept as true legal conclusions or unsupported conclusions of fact." *Bielanski v. Cty. Of Kane,* 550 F.3d 632 Cir. 2008). And "[t]hreadbare recitals of the elements of a cause of action, supported by merely conclusory statements do not suffice." *Iqbal*, 556 U.S. at 678.

Defendant also moves under Fed. R. Civ. P. 12(b)(1) alleging that Plaintiffs lack standing to sue. "Motions to dismiss under Rule 12(b)(1) are meant to test the sufficiency of the complaint, not to decide the merits of the case," and "[i]n the context of a motion to dismiss for lack of subject matter jurisdiction, [the court] accept[s] as true the well pleaded factual allegations, drawing all reasonable inferences in favor of the plaintiff[.]" *Center for Dermatology & Skin Cancer, Ltd. v. Burwell*, 770 F.3d 586, 588 (7th Cir. 2014). But "a plaintiff faced with a 12(b)(1) motion to dismiss bears the burden of establishing that the jurisdictional requirements have been met." *Burwell*, 770 F.3d at 588-89. "When a motion to dismiss is based on a lack of subject matter jurisdiction pursuant to Rule 12(b)(1), as well as other Rule 12(b)(6) defenses, the court should consider the Rule 12(b)(1) challenge first." *Rizzi v. Calumet City*, 11 F. Supp. 2d 994, 995 (N.D. Ill.

1998). If the court dismisses a plaintiff's complaint for lack of subject matter jurisdiction, the Rule 12(b)(6) defenses become moot and need not be addressed. *Id.* at 995.

II. Factual Background

Bradford-Scott is a technology and data service provider for over 280 credit unions across the country. (ECF No. 20, ¶¶ 2, 10, 14). In running its business, Bradford-Scott collects the personal identifiable information ("PII") of its current and former customers, including the PII of current and former customers of its institutional clients. (*Id.* ¶ 3). As for the PII here, Bradford-Scott collects and maintains those persons' names, social security numbers, birthdates, financial account information, credit card numbers, and debit card numbers. (*Id.* ¶ 26).

From May 19, 2023, until May 28, 2023, Bradford-Scott's system was hacked, and hackers had access to its customer's PII ("the Incident"). (*Id.* ¶ 23). Bradford-Scott detected the breach on July 2, 2023, and began notifying the affected customers in February 2024. (*Id.* ¶¶ 23-31). In its notice letter, Bradford-Scott admits that "certain files were likely copied from [its] network." (ECF No. 20-1). But Bradford-Scott had "no evidence… of any fraudulent use of any data as a result of [the Incident]" and remains unaware of any misuse to date. (*Id.*).

Plaintiff Webster is a former customer of StagePoint Federal Credit Union ("StagePoint"), Bradford-Scott's institutional client for data and technology services. (ECF No. 20, ¶¶ 46-47). In Plaintiff Webster's notice letter dated February 27, 2024, Bradford-Scott explains that his "name, and Social Security number and date of birth" was compromised. (ECF No. 20-1). Plaintiff Smith is also a former customer of a credit union that Bradford-Scott provided services for. (*Id.* ¶¶ 63-65). In his notice letter dated April 30, 2024, Bradford-Scott explained that his name, Social Security number, and financial account number were compromised. (*Id.* ¶ 67). And the 2024 Massachusetts Data Breach Notification Report indicates that customer's credit and debit card

numbers were compromised in the Incident too. (*Id.* ¶ 26). The notice letter offers a year of free credit monitoring services and encourages the recipient to "remain vigilant against incidents of identity theft and fraud by reviewing your accounts and monitoring your free credit reports." (*Id.* ¶ 68).

Plaintiffs filed suit in this forum seeking to certify a class of "[a]ll individuals residing in the United States whose PII was compromised in the Data Breach discovered by Bradford-Scott in July 2023, including those individuals who received notice of the breach." (*Id.* ¶ 98). Plaintiffs allege that the Incident occurred because Bradford-Scott "failed to adequately train its employees on cybersecurity and failed to maintain reasonable safeguards or protocols to protect [Plaintiffs'] PII." (*Id.* ¶ 5). Plaintiffs state that they have sustained damages—and will continue to suffer damages—in the form of monetary losses, lost time, anxiety, and emotional distress. (*Id.* ¶ 75). They also alleged that Plaintiffs "suffered or are at an increased risk of suffering: (a) loss of the opportunity to control how their PII is used; (b) diminution in the value of their PII; (c) compromise and continuing publication of their PII; (d) out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud; (e) lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by…preventing, detecting, contesting, and recovering from identity theft and fraud; (f) delay in the refund of tax refund monies; (g) unauthorized use of their stolen PII; and (g) continued risk to their PII[.]" (*Id.*).

Plaintiffs thus sued Bradford-Scott under theories of negligence (Count I), negligence per se under Section 5 of the Federal Trade Commission Act (Count II), breach of implied contract (Count III), invasion of privacy (Count IV), unjust enrichment (Count V), and breach of bailment (Count VI). (*Id.* at 23-37).

III. Discussion

Bradford-Scott seeks dismissal of all claims asserted in Plaintiffs' Amended Complaint. (ECF No. 25). It starts by broadly alleging that Plaintiffs lack an injury-in-fact sufficient to support standing. (*Id.* at 5-10). Bradford-Scott then focuses on Plaintiffs' causes of action individually and contends that they have failed to state a claim for each. The Court will first address Bradford-Scott's argument that Plaintiffs' alleged injuries do not confer standing and will then address each of Plaintiffs' substantive causes of action specifically below.

a. Standing

Article III of the Constitution limits the jurisdiction of federal courts to cases or controversies. U.S. Const. art. III, § 2; *Milwaukee Police Ass'n v. Flynn*, 863 F.3d 636, 639 (7th Cir. 2017). "There is no case or controversy if the plaintiff[s] lacks standing to challenge the defendant's alleged misconduct," *Diedrich v. Ocwen Loan Servicing*., LLC, 839 F.3d 583, 587 (7th Cir. 2016), and "the plaintiffs bear the burden of demonstrating that they have standing." *TransUnion, LLC v. Ramirez*, 594 U.S. 413, 430–431 (2021). This constitutional minimum is jurisdictional. *Exodus Refugee Immigr., Inc. v. Pence*, 165 F. Supp. 3d 718, 729 (S.D. Ind. 2016).

To establish Article III standing, a plaintiff must show that "(1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Silha v. ACT, Inc.*, 807 F.3d 169, 173 (7th Cir. 2015). To that end, Bradford-Scott argues that Plaintiffs case fails for lack of standing because "Plaintiffs have not suffered any actual injury, such as identity theft, actual misuse of their information, or economic harm" and "failed to allege any risk of future harm that can confer standing." (ECF No 25-1 at 5). Plaintiffs respond that the "time spent dealing with the aftermath of [Bradford-Scott's] failures is a concrete injury"

especially when partnered with Plaintiffs' intangible harms such as privacy harms, anxiety, fear, and frustration. (ECF No. 29 at 9). Having hoed this row previously in a similar context, the Court agrees with Plaintiffs that they have standing. *See McLaughlin v. Taylor Univ.*, 2024 WL 4274848, at *2-4 (N.D. Ind. Sept. 23, 2024).

The Court begins with Bradford-Scott's argument that the increased risk of future harm and anticipated mitigation costs are not injuries. Bradford-Scott relies on *TransUnion* for the notion that unmaterialized harms cannot confer standing:

> [I]f an individual is exposed to a risk of future harm, time will eventually reveal whether the risk materializes in the form of actual harm. If the risk of future harm materializes and the individual suffers a concrete harm, then the harm itself, and not the pre-existing risk, will constitute a basis for the person's injury and for damages. If the risk of future harm does *not* materialize, then the individual cannot establish a concrete harm sufficient for standing[.]

TransUnion, 594 U.S. at 436 (emphasis in original). And, indeed, "*TransUnion* makes clear that a risk of future harm, *without more*, is insufficiently concrete to permit standing to sue for damages in federal court." *Ewing v. MED-1 Solutions, LLC*, 24 F.4th 1146, 1152 (7th Cir. 2022) (emphasis added). But even the *TransUnion* Court recognized that "[v]arious intangible harms can…be concrete" and "[c]hief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuit in American Courts[,]" including, "for example, reputational harms, *disclosure of private information*, and intrusion upon seclusion." *TransUnion*, 594 U.S. at 425 (emphasis added) (citations omitted).

With that, it is hard to imagine more personal and private information than a person's social security number.[1] And, as one court put it, "[h]aving one's social security number stolen seems an

[1] Bradford-Scott relies on *Kim v. McDonald's USA* for the notion that Plaintiffs "cannot rely on their time and money spent in response to fears that are too speculative to support standing under Article III" when the fear of future harm was not certainly impending. 2022 WL 4482826, at *6 (N.D. Ill. Sept. 27, 2022). *Kim* is distinguishable because it involved only non-sensitive personal information unlike the social security numbers and financial information here.

obvious harm. If it were not a harm, why should [anyone] take any data security measures?" *Krupa v. TIC Int'l Corp.*, 2023 WL 143140, at *2 (S.D. Ind. Jan. 10, 2023). Here, hackers infiltrated Bradford-Scott's systems and stole Plaintiffs' PII, including their social security numbers and financial information. (ECF No. 20, ¶ 26). "If this were a bank robbery[,] no one would blink. It is a classic adversarial case." *Krupa,* 2023 WL 143140, at *2. Although *Krupa* couched this concept as common sense, Seventh Circuit case law is consistent.

About two decades ago, the Seventh Circuit held that plaintiffs "whose data has been compromised, but not yet misused," have suffered an injury-in-fact sufficient to confer standing, explaining that a plaintiff may have standing if the defendant's actions leave her under a "threat of future harm" or "increase[d] the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007). Following *Pisciotta*, the Supreme Court clarified that, to confer standing, a threatened injury must be "certainly impending" and cannot be based on mere "speculation" that a "highly attenuated chain of possibilities" might occur. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409-10 (2013). *Clapper* also acknowledged that plaintiffs need not demonstrate that their alleged harms are "literally certain" and "standing can be based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." *Id.* at 414 n.5.

Indeed, the Seventh Circuit has cautioned courts "not to overread *Clapper*," which addressed "speculative harm based on something that may not even have happened to some or all of the plaintiffs." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015). And when the plaintiffs are victims of an "alleged data theft" that has "already occurred," there is—

See Florence v. Ord. Express, Inc., 674 F. Supp. 3d 472, 481–82 (N.D. Ill. 2023) (distinguishing *Kim* because of the exposure of the plaintiffs' "social security and driver's license numbers").

unlike *Clapper*— "'no need to speculate as to whether . . . information has been stolen.'" *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966 (7th Cir. 2016) (quoting *Remijas,* 794 F.3d at 693). The Seventh Circuit has since acknowledged the concrete and imminent injuries data breach victims suffer.

Such victims, for example, are "at risk for both fraudulent charges and identity theft," even if those events have not yet manifested. *Lewert,* 819 F.3d at 967. In the same vein, they must "spen[d] time and effort monitoring both [their] card statements and [their] other financial information as a guard against fraudulent charges and identity theft." *Id*. And it seems that Bradford-Scott "implicitly acknowledge[s] this" by offering and encouraging credit monitoring services because "[i]t is unlikely that [Bradford-Scott] did so because the risk is so ephemeral that it can safely be disregarded." *Remijas,* 794 F.3d at 694. "Why else would hackers break in . . . and steal . . . private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those . . . identities." *Id.* at 693.

It is common sense that hackers steal personal information to profit from it, so there is no need "to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood that such injury will occur.'" *Lewert,* 819 F.3d at 966 (quoting *Remijas,* 794 F.3d at 693). Moreover, if the plaintiffs incur "mitigation expenses" to minimize the risk of harm from their stolen data being used for fraudulent purposes, these expenses qualify as "actual injuries" for standing purposes, because and to the extent that the data breach has "already occurred." *Id.* Then came *TransUnion*.

Lewert and *Remijas* predate *TransUnion.* The question thus becomes whether *TransUnion* undercuts these principles from *Remijas* and *Lewart*. Some district courts have answered in the affirmative. *See, e.g., Kim v. McDonald's USA, LLC,* 2022 WL 4482826 (N.D. Ill. Sept. 27, 2022).

These courts reason that mitigation-related injuries cannot confer standing because otherwise plaintiffs could "'manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'" *Id.* at * 6 (quoting *Clapper*, 568 U.S. at 416).

Other—and more—courts in this Circuit, however, answer that question in the negative. Those courts reason that a plaintiff who "has already lost time mitigating the risk of identity theft" after a data breach has suffered an injury-in-fact—namely, the lost time itself—and *TransUnion* is not to the contrary, as it simply "emphasized that whether a harm is concrete turns on whether it . . . already occurred." *Linman v. Marten Transp., Ltd.*, 2023 WL 2562712, at *3 (W.D. Wis. Mar. 17, 2023). "*TransUnion* held only that 'the mere risk of future harm, *standing alone*, cannot qualify as a concrete harm,' while holding open the possibility that 'the exposure to a risk of harm' might confer standing if it also 'causes a *separate* harm[.]'" *In re Mondelez Data Breach Litig.*, 2024 WL 2817489, at *3 (N.D. Ill. June 3, 2024). These courts thus do not consider an injury speculative just because it "relate[s] to the risk of harm." *Id.* at *3 (quoting *Linman*, 2023 WL 2562712, at *3). They conclude that "[t]he time spent mitigating the risk of identity theft is a separate harm from the risk of identity theft itself." *In re Mondelez Data Breach Litig.*, 2024 WL 2817489, at *3; *Linman*, 2023 WL 2562712, at *3; *see also Roper v. Rise Interactive Media & Analytics, LLC*, 2023 WL 7410641, at *4 (N.D. Ill. Nov. 9, 2023), *Florence v. Ord. Express, Inc.*, 674 F. Supp. 3d 472, 481 (N.D. Ill. 2023), *Doe v. Fertility Centers of Illinois, S.C.*, 2022 WL 972295, at *2 (N.D. Ill. Mar. 31, 2022); *Dusterhoft v. OneTouchPoint Corp*, 2024 WL 4263762, at *6 (E.D. Wis. Sept. 23, 2024). This Court agrees.

While "*TransUnion* marked a shift in the Court's standing jurisprudence[,]" the Seventh Circuit has yet to cut the legs from under *Remijas* and *Lewart*. *See Dinerstein v. Google, LLC*, 73

F.4th 502, 516 (7th Cir. 2023) (While "[*Remijas* and *Lewart*] predate *TransUnion*…that is not to say that they are no longer authoritative[.]"); *Dusterhoft*, 2024 WL 4263762, at *6 (In light of *Remijas* and *Lewert*, "Plaintiffs' alleged mitigation efforts taken in the face of impending harm remain sufficient under Seventh Circuit law."). And with *Remijas* and *Lewart* still standing, so too do Plaintiffs here have standing.

Bradford-Scott does not dispute that the Incident "already occurred." And Plaintiffs are victims of the data breach and now face the risk of identity theft. Some district courts in this Circuit have found that alone sufficient to confer standing. *See In re Mondelez Data Breach Litig.*, 2024 WL 2817489, at *3 (Reasoning that "a plaintiff who is the victim of a data breach has suffered a harm that has 'already occurred,' and that harm satisfies the injury-in-fact requirement by putting him at a 'substantial risk' of further 'future harm[.]'"). In light of *TransUnion*, the Court believes that alone would be insufficient because the Supreme Court requires a "separate harm" in addition to the risk of identity theft itself. But Plaintiff Webster plausibly alleges that, in the wake of the breach, he has "spent…significant time and effort monitoring his accounts" to combat identity theft. (ECF No. 20, ¶ 55). Plaintiff Smith plausibly alleges that he "made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach" and "signing up for credit monitoring and identity theft protection services." (*Id.* ¶ 68). And they did so at Bradford-Scott's direction. (*Id.*). To the extent that *TransUnion* requires a "separate harm" apart from the data breach itself, Plaintiffs undertook mitigation efforts to combat a harm that was imminent or certainly impending. They thus have standing.

Having found as much, the Court need not decide whether Plaintiffs' other alleged injuries are sufficient. *Linman*, 2023 WL 2562712, at *3 (Because "time spent mitigating the risk of identity theft is a concrete harm that gives him standing to sue for damages related to the breach,

so the court need not consider whether the other alleged injuries are sufficient[.])". While Plaintiffs may ultimately have trouble proving a causal connection between their alleged harms and the data breach, the Amended Complaint sufficiently alleges that Plaintiffs undertook mitigation efforts to combat a harm that was imminent or certainly impending in the wake of the Incident.

b. Negligence (Count I)

Under Indiana law, common law negligence claims consist of three elements: "(1) duty owed to plaintiff by defendant, (2) breach of duty by allowing conduct to fall below the applicable standard of care, and (3) compensable injury proximately caused by defendant's breach of duty." *Bader v. Johnson*, 732 N.E.2d 1212, 1217 (Ind. 2000). Bradford-Scott moves to dismiss Plaintiffs' common law negligence claim under Rule 12(b)(6) because: (1) "Indiana does not recognize a duty to protect information"; (2) "Plaintiffs do not properly plead…that they have suffered any cognizable injury"; and (3) Plaintiffs' negligence claim is barred by the economic loss doctrine. The parties thus dispute whether a common-law negligence duty applies, whether there are compensable damages, and—if there are damages—whether they are precluded by the economic loss rule. The Court addresses each issue in turn.

Starting with the first element, the issue is whether Bradford-Scott owed a duty to protect Plaintiffs' PII. "[B]usinesses have the common-law duty to exercise ordinary and reasonable care in the conduct of their operations . . . for the safety of others whose injuries should reasonably have been foreseen or anticipated." *WEOC, Inc. v. Niebauer*, 226 N.E.3d 771, 778 (Ind. 2024). "Whether a duty exists is generally a question of law for the court." *Id.* No duty, then no negligence claim. *Jaffri v. JPMorgan Chase Bank, N.A.*, 26 N.E.3d 635, 638 (Ind. Ct. App. 2015) ("A defendant cannot be found negligent where there is no duty to the plaintiff.").

Bradford-Scott argues that Indiana law does not recognize a common law duty to protect

Plaintiffs' PII, relying on *Aspen Am. Ins. v. Blackbaud, Inc.*, 2023 WL 3737050, at *4 (N.D. Ind. May 31, 2023) ("Indiana state statutes support a finding that Indiana law does not recognize a common law duty to compensate the public for inconvenience or potential harm caused by data exposure."). (ECF No. 13 at 11). Indeed, *Apsen* supports such a finding. But in *Apsen,* "neither party cite[d] to any cases from Indiana supporting that such a duty exists," 624 F. Supp. 3d 982, 998, so the court relied on *Pisciotta v. Old Nat'l Bancorp*, which interpreted Indiana's then-data-breach statute. 499 F.3d 629 (7th Cir. 2007) ("[Indiana's data-breach statute] imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow [a breach].").

"Although *Pisciotta* interpreted the Indiana data-breach statute, it was decided before Indiana cases permitting common law data-breach negligence claims." *Johnson v. Nice Pak Prods., Inc.*, 2024 WL 2845928, at *4 (S.D. Ind. June 5, 2024). The *Johnson* court, addressing a similar issue in the employee-to-employer context, reasoned that "generally, employees reasonably expect their employers to keep their personal information safe. Even in the era before digital recordkeeping, if an employer kept its employees' Social Security numbers in an unlocked box on the sidewalk for anyone to take, no one would question that the employer would be negligent." *Id.* at *13. And Indiana common law has adapted to the digital age. *See, e.g.*, *Paul,* 2023 WL 5153147, at *7 (holding that Defendant owed a duty to protect Plaintiff's PII in a reasonably secure manner); *In re Eskenazi Health Data Incident Litig.*, 2022 WL 20505180, at *11 (same). This Court is already in line. *See McLaughlin,* 2024 WL 4274848, at *5 ("Taylor took the affirmative act of collecting and maintaining students' and employee's information… [so it] assume[d] a duty to maintain that information in a reasonably secure manner.").

Bradford-Scott seeks to distinguish the aforementioned authority because those cases

concerned plaintiffs that had a direct relationship with the defendant through an employer-employee or consumer-business relationship. (ECF No. 31 at 7-8). Indeed, Bradford-Scott obtained Plaintiffs Webster and Smith's PII from their credit unions; not from Plaintiffs themselves. And perhaps Plaintiffs were not even aware of who Bradford-Scott was before the incident. Those points are well taken and will have consequences below. But they make little (if any) difference regarding Plaintiffs' negligence claim.

Indiana has adopted the Restatement (Second) of Torts section 302, *see Gariup Constr. Co. v. Foster*, 519 N.E.2d 1224, 1228 (Ind. 1988), which imposes a duty on anyone who affirmatively acts to act reasonably. "[B]y taking the affirmative act of collecting the PII, [Bradford-Scott] assumes a duty to maintain that information in a reasonable manner." *Paul*, 2023 WL 5153147, at *7 (citing Restatement (Second) of Torts section 302). That duty "includes protecting against unauthorized misappropriation of the PII because the general harm of unauthorized disclosure of the sensitive PII could reasonably be expected to occur against the class of persons such as [Plaintiffs] who provided their PII to [Bradford-Scott.]" *Id.* (citing *Rogers v. Martin*, 63 N.E.3d 316, 325 (Ind. 2016)). Bradford-Scott owes this duty to all whose "injuries should reasonably have been foreseen or anticipated," *Niebauer*, 226 N.E.3d at 778, whether they have a direct relationship or not. Put differently, if you are going to collect it, you better (reasonably) protect it.

Plaintiffs plead that they, or their third-party agents, entrusted Plaintiffs' PII to Bradford-Scott as a necessary part of obtaining services and with the understanding that it would not be disclosed to unauthorized third parties. (ECF No. 20, ¶¶ 109, 117). And Plaintiffs plead that Bradford-Scott owed a duty to Plaintiffs "because it was foreseeable that [Bradford-Scott's] failure—to use adequate data security in accordance with industry standards for data security—

would compromise their PII in a data breach. And here, that foreseeable danger came to pass." (*Id.* ¶ 110). The Court holds that Bradford-Scott owed a duty to Plaintiffs to keep their PII safe and that Plaintiffs adequately pled that element in their Amended Complaint.

Bradford-Scott next argues that Plaintiffs fail to plead any cognizable loss that would sustain a negligence claim. It argues that Plaintiffs "asserted injuries are boilerplate and speculative allegations premised on potential future harm, mitigation efforts to avoid identity theft, and loss in value of their personal information." (ECF No. 25-1 at 14). While it is apparent that Bradford-Scott views standing and cognizable injury as distinct concepts, the two "can be difficult to keep separate[.]" *Bond v. United States*, 564 U.S. 211, 218-19 (2011). "A plaintiff to have standing must have an injury, and a plaintiff to have an Indiana cause of action for negligence…must have an injury." *Krupa*, 2023 WL 143140, at *1 (internal citations omitted). Bradford-Scott cites no in-circuit authority to support that the standard for injury-in-fact under Article III is different from that of a compensable injury under Indiana law. And like this Court and others in this Circuit have said, "the Court sees no difference as applied here". *McLaughlin*, 2024 WL 4274848, at *5; *See also Johnson.*, 2024 WL 2845928, at *14.

Starting with its argument that the increased risk of future harm and anticipated mitigation costs are not injuries, Bradford-Scott relies heavily on *Pisciotta*, 499 F.3d 629. In *Pisciotta*, the issue was "whether Indiana would consider that the harm caused by identity information exposure . . . constitutes *an existing compensable injury and consequent damages* required to state a claim for negligence or for breach of contract." *Id.* at 635 (emphasis in original). At that time, the answer was no. *Id.* But the Seventh Circuit and Indiana courts alike have since steadily veered off *Pisciotta*'s path. *See, e.g.*, *McLaughlin*, 2024 WL 4274848, at *5 (reasoning that courts have been "chipping away at *Pisciotta*'s commands" and concluding that "the increased risk of identity theft

that Plaintiffs now face and the costs to mitigate those risks are cognizable injuries"); *Paul*, 2023 WL 5153147, at *7; *In re Eskenazi Health Data Incident Litig.*, 2022 WL 20505180, at *11; *Remijas*, 794 F.3d at 694; *Lewert*, 819 F.3d at 967.

Again, *Remijas* and *Lewert* recognize the concrete and imminent injuries that data breach victims such as Plaintiffs face. *Remijas, supra*, at 693-94; *Lewert, supra*, at 966-67. And although those cases concerned Article III's standing requirement, Indiana law on compensable injuries is consistent. For example, Indiana law explicitly allows as damages "the value of [lost time]." Ind. Model Civ. Jury Inst. 703(3) (brackets in original); *See also Johnson*, 2024 WL 2845928, at *14. And at least one Indiana Court found that further proceedings are necessary "to determine the extent to which those damages can be compensated as arising from the Data Breach at issue in [that] case." *Paul*, 2023 WL 5153147, at *6. That said, the Court finds that the increased risk of identity theft that Plaintiffs now face and the costs to mitigate those risks are cognizable injuries and adequately plead. In line with *Paul*, the extent to which those injuries can be compensated remains to be seen.

As for Plaintiffs' emotional distress and anxiety related damages, such damages are also plausible and adequately plead. Having found that Plaintiffs' mitigation efforts and the accompanying time spent is a cognizable injury under Indiana law, the emotional toll stemming from the Incident too is cognizable. But Plaintiffs' alleged damages through the diminished value of their PII gives the Court a moment of pause.

Although Bradford-Scott spent little effort developing the argument that the diminished value of PII is not recoverable under Indiana law, it did raise it. (ECF No. 25-1 at 14). Such damages are not compensable. In *Silha v. ACT, Inc.*, the Seventh Circuit affirmed the Illinois District Court's "reject[ion of] the claimed injury of diminished value of PII because Plaintiffs

failed to 'allege that they have the ability to sell their personal information or that Defendants' conduct foreclosed them from entering into a 'value for value transaction' relating to their PII." 807 F.3d 169, 172 (7th Cir. 2015). While PII does have value, it is hard to see how the value of Plaintiffs' PII has been diminished. Indeed, Plaintiffs fail to "explain how the hackers' possession of . . . information has diminished its value, nor d[o] [they] assert that [they] would ever actually sell [their] own personal information." *Khan v. Child. Nat'l Health Sys.*, 188 F. Supp. 3d 524, 531 (D. Md. 2016) (rejecting diminished value of PII theory in the standing context). Instead, Plaintiffs rely on general allegations highlighting PII's value on the black market. (ECF No. 20, ¶ 76). Nothing suggests that Plaintiffs' PII lost value in legitimate markets. Nor does anything suggest that Plaintiff cannot continue to enter value-for-value transactions using their PII on such markets. *See Griffey v. Magellan Health Inc*., 562 F. Supp. 3d 34, 46 (D. Ariz. Sept. 27, 2021) ("[W]ithout identifying a market in which they can or could and intend or intended to sell their information, Plaintiffs here fail to demonstrate a loss in value of their PII or PHI.").

From this Court's research, just one Indiana court has opined on the issue and said only that "the diminution of value in the PII has been deemed a credible harm by at least some federal courts." *In re Eskinazi*, 2022 WL 20505180, at *4 (citing *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460-62 (D. Md. 2020); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1034 (N.D. Cal. 2019)). The out-of-circuit cases relied upon on *In re Eskanazi* do not speak to Indiana law, and the Seventh Circuit presents contrary authority which the Court follows. *See Silha*, 807 F.3d at 172. The diminished value of Plaintiffs' PII is simply "too speculative" to establish a cognizable injury. That aside, Plaintiffs may pursue their other theories of recovery.

Lastly, Bradford-Scott argues that Plaintiffs' negligence claim is barred by the economic

loss doctrine. (ECF No. 25-1 at 15). Under Indiana law, "a defendant is not liable under a tort theory for any purely economic loss caused by its negligence." *U.S. Bank, N.A. v. Integrity Land Title Corp.*, 929 N.E.2d 742, 745 (Ind. 2010). "[C]ontract is the only available remedy where the loss is solely economic in nature. . . in the absence of damage to other property or person." *Aspen Am. Ins. v. Blackbaud, Inc.*, 624 F. Supp. 3d 982, 1002 (N.D. Ind. 2022) (quoting *Gunkel v. Renovations, Inc.*, 822 N.E.2d 150, 152 (Ind. 2005)). But "the economic loss doctrine's preclusive effect must yield if the plaintiff has set forth *any set of circumstances* under which it would be entitled to relief—a relatively low bar." *Residences of Ivy Quad Unit Owners Ass'n, Inc. v. Ivy Quad Dev., LLC*, 179 N.E.3d 977, 983 (Ind. 2022) (emphasis added).

Plaintiffs allege more than purely economic losses here. Their alleged damages include—among other things—lost time, anxiety, embarrassment, humiliation, frustration, and emotional distress. (ECF No. 20, ¶¶ 75, 126). In *Residences*, the Indiana Supreme Court held that, although the economic loss doctrine may preclude the plaintiffs' negligence claim as the facts developed, dismissal was inappropriate because the plaintiffs' alleged damages were not purely economic. 79 N.E.3d at 982; *See also Johnson*, 2024 WL 2845928, *16 ("In any event, at least some of the harms experienced by the Plaintiffs are not solely economic, such as lost time and worry"). Plaintiffs plead similarly here and have set forth a set of circumstances under which tort law would be the appropriate remedy. Because Plaintiffs have plausibly alleged non-economic harms, dismissal would be inappropriate at this juncture.

In short, Plaintiffs' Amended Complaint checks all the boxes for a negligence claim under Indiana law, and the economic loss doctrine does not warrant dismissal. The Court thus DENIES Bradford-Scott's Motion to Dismiss as to Plaintiffs' negligence claim.

c. Negligence Per Se (Count II)

Plaintiffs also allege negligence per se under Section 5 of the Federal Trade Commission Act ("FTCA"). (ECF No. 20, ¶¶ 129-38). The FTCA prohibits "unfair…practices in or affecting commerce." 15 U.S.C. § 45(a)(1). Plaintiffs allege that this provision imposes a duty on Bradford-Scott "to use fair and adequate computer systems and data security practices to safeguard Plaintiffs'…PII." (ECF No. 20, ¶ 130). Bradford-Scott moves to dismiss Plaintiffs' negligence per se claim because the FTCA does not provide a private right of action. (ECF No. 25-1 at 15-17). In the alternative, it contends that Plaintiffs fail to plead that any alleged violation of the FTCA proximately caused Plaintiffs' injuries. (*Id.*).

Plaintiffs respond that they "have not asserted a cause of action for violation of the FTC Act, rather they are using the Defendant's violation of the FTC Act to inform the existence and scope of Defendant's duty to safeguard personal information." (ECF No. 29 at 17). Bradford-Scott, in reply, argues that this a run-around attempt by Plaintiffs to assert a private cause of action under the FTCA. (ECF No. 31 at 8-9). Indeed, the difference between asserting a private right of action and a claim for negligence per se is a common point of contention and confusion. *See Gresser v. Reliable Exterminators, Inc.*, 160 N.E.3d 184, 191 (Ind. Ct. App. 2020) ("[T]hese two forms of tort claim are often confused[.]").

Negligence per se claims and private right of action claims, though similar, are distinct. *Stachowski v. Est. of Radman*, 95 N.E. 3d 542, 545 (Ind. Ct. App. 2018) ("whether a statute or ordinance confers a 'private right of action'" is "a concept that is related to but distinct from the doctrine of negligence per se."). A private right of action assumes that an alleged "violation of a statute or ordinance gives rise to civil liability even in the absence of a common-law duty." *Id*. Negligence per se, on the other hand, "assumes the existence of a common-law duty of reasonable care, and the court is asked to adopt the standard of conduct set forth in a statute or ordinance . . .

as the standard of conduct required under that preexisting duty, so that a violation of the statute or ordinance serves to satisfy the breach element of a negligence action." *Id.* at 544. Indeed, negligence per se claims "differ in that a violation of certain statutes or ordinances serves to satisfy the breach element." *Johnson*, 2024 WL 2845928, at *5 (quoting *WEOC, Inc. v. Niebauer*, 226 N.E.3d 771, 778 (Ind. 2024)).

With this backdrop, an "unexcused violation of a statutory duty constitutes negligence per se if the statute or ordinance is intended to protect the class of persons in which the plaintiff is included and to protect against the risk of the type of harm which has occurred as a result of its violation." *Erwin v. Roe*, 928 N.E.2d 609, 619 (Ind. Ct. App. 2010) (internal quotations omitted). Thus, "[t]he question for the jury is not whether the [FTCA] was violated but whether [Defendant] breached [its] duty to protect [Plaintiffs'] PII by failing to meet the standard of care articulated in the [FTCA]." *Paul*, 2023 WL 5153147, at *9.

The Court agrees that Plaintiffs are not pursuing a private cause of action for violations of the FTCA; they assert that Bradford-Scott's violations of those statutes evince a breach of its duty to protect Plaintiffs' PII. (ECF No. 1, ¶¶ 129-38). The FTCA prohibits unfair acts that affect commerce. 15 U.S.C. § 45. "Data breaches affect commerce, and Plaintiffs benefit from protections against the kinds of harms that proper data security would avoid." *Johnson*, 2024 WL 2845928, at *18. "[T]he non-existence of [a private right of action] under…the [FTCA]…does not preclude Plaintiffs' claims." *In re Eskanazi*, 2022 WL 20505180, at *24. And while Bradford-Scott argues that the courts in *Paul* and *Johnson* "centered their analysis on the parties' employer-employee relationship" (ECF No. 31 at 9), *Paul* explicitly stated that the FTCA "could apply to protect employee's information as well" as "consumers[']" information. 2023 WL 5153147, at *8. And *Johnson*'s entire analysis of negligence per se did not so much as mention an employer-

employee relationship. 2024 WL 2845928, at *5-6.

The Court also finds Bradford-Scott's argument on proximate cause unavailing. Plaintiffs allege that Bradford-Scott "violated its duty under Section 5 of the [FTCA] by failing to use reasonable measure to protect PII" and "[a]s a direct and proximate result…Plaintiffs…have suffered and will continue to suffer numerous injuries." (ECF No. 20, ¶¶ 133, 138). Proximate cause is almost always a question of fact for the factfinder. *Smith v. Walsh Constr. Co. II, LLC*, 95 N.E.3d 78 (Ind. Ct. App. 2018) (citing *Megenity v. Dunn*, 68 N.E.3d 1080, 1083 (Ind. 2017)). Plaintiffs plead that Bradford-Scott's alleged breach of its duties under the FTCA proximately caused their harm. And, as stated above, Plaintiffs allege viable harms caused by such breaches. The Court must go outside the Amended Complaint to determine whether these alleged breaches did, in-fact, cause Plaintiffs' injuries. Summary Judgment is the appropriate mechanism for such a determination.

That said, "'the FTCA can serve as the basis of a negligence per se claim[,]'" *McLaughlin*, 2024 WL 4274848, at *7 (quoting *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 760-61 (C.D. Ill. 2020), and Plaintiffs have plausibly alleged such a claim. The Court thus DENIES Bradford-Scott's Motion to Dismiss as to Plaintiffs' negligence per se claim.

c. Breach of Implied Contract (Count III)

An Indiana breach of contract claim consists of three elements: "(1) a contract existed, (2) the defendant breached the contract, and (3) the plaintiff suffered damage as a result of the defendant's breach." *Trustees of Indiana University v. Spiegell*, 186 N.E.3d 1151, 1158 (Ind. Ct. App. 2022) (citation and quotation omitted). "The elements of an implied-in-fact contract are the same as an express contract: offer, acceptance, and consideration." *Wakley v. Sustainable Loc. Foods LLC*, 2017 WL 1880814, at *3 (S.D. Ind. May 9, 2017) (internal citations omitted). Unlike

express contracts, "[a]n implied in fact contract refers to the class of obligations which arises from mutual agreement and intent to promise, when the agreement and promise have simply not been expressed in words." *McCart v. Chief Exec. Officer in Charge, Indep. Fed. Credit Union*, 652 N.E.2d 80, 85 (Ind. Ct. App. 1995). Accordingly, "a contract implied in fact arises out of acts and conduct of the parties, coupled with a meeting of the minds and a clear intent of the parties in the agreement." *Id.*

Although no written agreement was executed, Plaintiffs argue that a contract existed through Bradford-Scott's Privacy Policy and advertisements. (ECF No. 29 at 18-25). Bradford-Scott argues that "Plaintiffs fail to assert any allegations establishing mutual assent or clear intent between the parties" and, "[w]ithout a meeting of the minds, there is no enforceable contract." (ECF No. 25-1 at 18). In a data breach case, this Court previously held that it was premature to dismiss the plaintiffs' claim for breach of implied contract when the defendant's privacy policy supported such an agreement in the "employer-to-employee" and "university-to-student" contexts. *See McLaughlin*, 2024 WL 4274848, at *8-9 ("Whether the relationship is employer-to-employee or university-to-student, there is a general understanding that PII should be kept private. Such an understanding is plausibly implicit in the terms of Plaintiffs' employment or educational contracts."). And *Archey v. Osmose Utilities Servs., Inc.*, 2022 WL 3543469, *4 (N.D. Ill. Aug. 18, 2022), which both parties cite in support of their positions, stated that an implied contract may exist "in the employee-employer data breach context…when the plaintiffs were able to point to some document, expression, or action of the employer which indicated an intention to protect the employee's personal information." But that is not the relationship between Plaintiffs and Bradford-Scott. Neither named Plaintiff alleges that they had a direct relationship with Bradford-Scott. And, unlike Plaintiffs' negligence claim, the extra degree of separation here is fatal.

The Amended Complaint reveals that Plaintiffs could not have reached "meeting of the minds" with Bradford-Scott. Plaintiffs were not employees or direct customers of Bradford-Scott; rather, Bradford-Scott received Plaintiffs' PII through their credit unions. Plaintiffs had no direct dealings with Bradford-Scott. Nor do Plaintiffs allege that they knew of or read Bradford-Scott's Privacy Policy and advertisements—on which their breach of contract claim rests—when the Incident occurred. Moreover, they do not plead that they knew of Bradford-Scott's existence at all before the Incident. *See Doe v. Fertility Centers of Ill.*, 2022 WL 972295, at *4 (N.D. Ill. Mar. 31, 2022) (dismissing implied contract claim in a data breach case where the plaintiff was unaware of the company whose data breach allegedly caused disclosure of the plaintiff's sensitive medical information).

Therein lies the problem for Plaintiffs. "Plaintiffs had no direct dealings with [Bradford-Scott] and were [likely] unaware of [Bradford-Scott's] existence until they received notice from [it] of the Data Breach. They thus could not have reached any implied understanding with [Bradford-Scott]." *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 591 (N.D. Ill. 2022). As plead, the Court is confident that there could not have been a meeting of the minds sufficient for the existence for an implied contract. Put differently, where—as here—the parties had no direct dealings and the complaint does not even support that the plaintiff knew that the defendant existed before a data breach, there can be no implied contract.

Plaintiffs' authority to the contrary is not convincing. First, although *Archey* suggests that a privacy policy could evince the existence of an implied contract, the court couched its findings to the employee-employer context. 2022 WL 3543469, *4. Again, such is not the case here. Alternatively, Plaintiffs argue that *Archey* is unpersuasive as it interpreted Illinois law on implied contracts and "Indiana case law already provides clear guidance for data breaches." (ECF No. 29

at 19). Plaintiffs cite *In re Eskenazi* for the notion that "Plaintiffs' entrusting Defendant with their PII . . . creates an inference that Defendant would then safeguard this information against theft." 2022 WL 20505180, at *7. But in that case, the plaintiff had a direct relationship with the defendant. *In re Eskenazi*, 2022 WL 20505180, at *1 (the plaintiffs were "patients, employees, and providers" of the defendant). They also cite *Krupa* in which the court denied dismissal and stated that "[plaintiff] alleges that [defendant] held his personal data subject to a shared understanding that it would remain confidential, but . . . exposed that data to hackers." 2023 WL 143140, at *5. But the only issues that court was tasked with was whether the plaintiff sustained an injury sufficient to confer standing and sustain an Indiana cause of action. *Id.* at *1. *Krupa* did not analyze the parties' relationship and whether there was a meeting of the minds. That said, Indiana law has not provided clear guidance in this context and Plaintiffs' authority is readily distinguishable.

How can there be a meeting of the minds when the parties have no direct relationship? Some circumstance might exist. But what about when the plaintiff does not know that the defendant existed before a data breach? Seems commonsensical: in such a situation, there cannot be a meeting of the minds. In sum, the parties have no direct relationship, Plaintiffs do not allege that they knew of or read Bradford-Scott's Privacy policy and advertisements, and there is no allegation that Plaintiffs knew of Bradford-Scott's existence before the Incident. The Court thus GRANTS Bradford-Scott's Motion to Dismiss as to Plaintiffs' breach of contract claim.

d. Invasion of Privacy (Count IV)

Invasion of privacy claims encompass four theories of wrongdoing: (1) intrusion upon seclusion; (2) appropriation of a person's name or likeness; (3) public disclosure of private facts; and (4) publicity placing a person in a false light. *See Pucillo v. Nat'l Credit Sys., Inc.*, 66 F.4th 634, 639 (7th Cir. 2023). Plaintiffs' claim is for public disclosure of private facts which, under

Indiana law, consists of four elements: "(1) the information disclosed must be private in nature; (2) the disclosure must be made to the public; (3) the disclosure must be one that would be highly offensive to a reasonable person; and (4) the information disclosed is not of legitimate public concern." *Cmty. Health Network, Inc. v. McKenzie*, 185 N.E.3d 368, 382 (Ind. 2022). Bradford-Scott asserts that Plaintiffs' Amended Complaint fails to allege the second element, also known as the publicity element.

Bradford-Scott argues that Plaintiffs' claim should be dismissed because "Plaintiffs conceded that [Bradford-Scott] did not disclose their [PII], but that it was instead stolen by third-party cybercriminals." (ECF No. 31 at 12). It also contends that "Plaintiffs do not offer any allegation that their information was publicly divulged." (*Id.*). Plaintiffs rely on *Z.D. v. Cmty. Health Network, Inc.*, 217 N.E.3d 527, 533-36 (Ind. 2023), where the Indiana Supreme Court held that the "public-disclosure tort is not an intentional tort" and "disclosure to one person may, depending on the surrounding facts and circumstances, satisfy the tort's publicity element." (ECF No. 29 at 21). And they believe they their "allegations satisfy their pleading burden" because Bradford-Scott "disclosed private information…to cybercriminals (and upon information and belief, to the Dark Web)." (*Id.* at 21-22).

This Court has been critical of extending Indiana's public-disclosure tort to data breach cases such as this. *See McLaughlin,* 2024 WL 4274848, at *10 ("In analyzing the facts of *Z.D.*, the Court agrees that Indiana's public-disclosure tort should not be wrapped around data breach cases such as this."). And the Court does not construe Bradford-Scott's argument to mean that the tort requires some mental state. Indeed, public-disclosure cases "uniformly hold that the publicity requirement is met only if said publicization is attributable to the defendant—i.e., defendant must have caused, precipitated or permitted the publicity." *Z.D.*, 217 N.E.3d at 536 (quoting David A.

Elder, Privacy Torts § 3.3 (2022)). With this in mind, Bradford-Scott appears to argue that there is no public disclosure attributable to it.

Z.D. was not a data breach case and the Court agrees with Bradford-Scott that the facts of *Z.D.* do not support an extension of Indiana's public-disclosure tort to such cases. Here's why:

> In *Z.D.*, the plaintiff received medical care from one of the defendant's facilities. *Id.* at 530. After her visit, the defendant's employee tried to call the plaintiff to discuss her health matters. *Id.* Unable to reach the plaintiff, the employee prepared a letter documenting *Z.D.*'s private health information. *Id.* Although the letter was properly addressed, the envelope in which it was placed was addressed to the wrong person and mailed to that person. *Id.* That person ended up being a teenager who attended the same school as the plaintiff's daughter. *Id.* When the improper person received the letter, she posted the letter to Facebook. *Id.*
>
> From this, the Indiana Supreme Court determined that "[t]he public-disclosure tort embodies dual imperatives, neither of which are served by imposing an intent requirement." *Id.* at 534. "First, from individuals and entities alike, the tort demands protection for private information" and "serves to deter the unauthorized disclosure of private information." *Id.* Such deterrence may be achieved by implementing security measures. *Id.* Recognizing that "such measures may fall short[,]" the second imperative is "when failures occur, injured individuals deserve a remedy." *Id.*
>
> Although these dual imperatives may be served by allowing the cause of action here, the Court doubts that the Indiana Supreme Court would stretch its bounds so far. *See Republic Servs. of Indiana Ltd. P'ship v. Coe Heating & Air Conditioning, Inc.*, 700 F. Supp. 3d 676 (N.D. Ind. 2023) ("[F]ederal district courts must act as a prognosticator of what a state court would decide when a state's Supreme Court is silent."). An alteration in the facts of *Z.D.* demonstrates why. Say, for example, the defendant's employee properly addressed the envelope and placed it in a safe at the defendant's facility. Overnight, a third-party burglar broke into the facility, cracked the safe, and stole the letter. The burglar then posted that letter to Facebook. That does not sound like the defendant publicly disclosed the plaintiff's private health information. If anything, that sounds like negligence.

McLaughlin, 2024 WL 4274848, at *11. Such is the case here and the Court has already permitted Plaintiffs to proceed on their negligence claim. A sophisticated third-party cyberattack is a far cry from a mislabeled envelope.

Moreover, Plaintiffs' Amended Complaint does not provide a basis for the Court to believe

that Plaintiffs' PII was communicated in a manner that is sure to reach the public. "The information must be communicated in a way that either reaches or is sure to reach the public in general or a large enough number of persons such that the matter is sure to become public knowledge." *McKenzie*, 185 N.E.3d at 382. Plaintiffs simply plead that "on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the dark web." (ECF No. 20, ¶ 168). Although the Court must take this statement as true under Rule 12(b)(6), "a formulaic recitation of a cause of action's elements will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 545 (2007). The Amended Complaint fails to establish that Plaintiffs' PII has reached the public at large. Nor does the Amended Complaint suggest that Plaintiffs' PII will *surely* become public knowledge. All told, Plaintiffs' Amended Complaint is insufficient to sustain a claim for public disclosure of private facts.

The Court thus GRANTS Bradford-Scott's Motion to Dismiss Plaintiffs' claim for invasion of privacy.

e. Unjust Enrichment (Count V)

Bradford-Scott next argues that Plaintiffs' claim for unjust enrichment must fail because "Plaintiffs did not confer any benefits upon [Bradford-Scott] at its request, did not expect any kind of payment, and have not established anything 'unjust[.]'" (ECF No. 25-1 at 22). Plaintiffs respond that they plausibly allege that "they conferred a benefit" through their "PII (and/or payment)" with the understanding that "[Bradford-Scott] would use adequate security measures." (ECF No. 29 at 20). It is Plaintiffs' position that "[Bradford-Scott] should not be permitted to retain the full value of the PII (and/or payment) . . . because [it] failed to adequately protect their PII." (*Id.*).

Under Indiana law, unjust enrichment claims have three elements: "(1) a benefit conferred upon another at the express or implied request of this other party; (2) allowing the other party to

retain the benefit without restitution would be unjust; and (3) the plaintiff expected payment." *Woodruff v. Ind. Fam. & Soc. Servs. Admin.*, 964 N.E.2d 784, 791 (Ind. 2012). "Put another way, 'a plaintiff must establish that a measurable benefit has been conferred on the defendant under such circumstances that the defendant's retention of the benefit without payment would be unjust. One who labors without an expectation of payment cannot recover in quasi-contract.'" *Id.*

Plaintiffs rely on *In re Eskanazi* to support their position that dismissal is improper as the pleading stage. 2022 WL 20505180. There, the Indiana trial court declined to dismiss the plaintiffs' unjust enrichment claim because "Plaintiffs [alleged] that data security from Defendant was part of their overall payment for medical services. By allegedly failing to secure Plaintiffs PII and PHI but still retaining all of the overall payments, the Court concludes that Defendant may have possibly retained the benefit of Plaintiffs' full payments unjustly." *Id.* at *9. But Plaintiffs' reliance on *In re Eskanazi* is inapposite. The plaintiffs in *In re Eskanazi* survived dismissal because their "overall payment *for medical services*…[was] alleged to have been" directed to data security, such that the defendant "may have retained the full value" of those payments unjustly. *Id.* If Plaintiffs provided anything here, it was simply their PII. They cannot rely on *In re Eskanazi* as neither named Plaintiff provided payment to Bradford-Scott.

To that end, Plaintiffs press that even a benefit conferred through a third-party can support an unjust enrichment claim. *See Bloombank v. United Fid. Bank F.S.B.*, 113 N.E.3d 708, 729 (Ind. Ct. App. 2018) ("[T]his Court has allowed a plaintiff to recover against a defendant for unjust enrichment even when it was a third party that conferred the benefit on the defendant and the defendant did not request the benefit from the plaintiff."). But that argument too misses the mark. The issue is not whether Plaintiffs' indirect conferral of their PII to Bradford-Scott through their credit unions is a benefit. The issue is whether Plaintiffs' PII serves as a benefit at all.

Plaintiffs must establish not only that the PII is a "benefit," but that it is a "measurable benefit." *See Woodruff*, 964 N.E.2d at 791 ("[A] plaintiff must establish that a measurable benefit has been conferred on the defendant…"). While Indiana recognizes data as property which this Court concedes has *some* value, it is hard to see how Bradford-Scott benefited from Plaintiffs' PII other than benefits incidental to running its business operations. From the Amended Complaint, it appears that Bradford-Scott provided software for Plaintiffs' credit unions. (ECF No. 20, ¶¶ 14-15). It is difficult (perhaps, impossible) to implement new software for a credit union if Bradford-Scott could not identify the credit union's customers through their PII. As applied here, "[t]he PII is better understood as necessary to conduct business operations, not a good whose inherent value was extracted by [Bradford-Scott]." *Johnson*, 2024 WL 2845928, at *25-26 (dismissing unjust enrichment claim). The Court is confident that the PII does not cast a measurable benefit here.

Moreover, even if the payments by Plaintiffs' credit unions to Bradford-Scott supplied a measurable benefit where Plaintiffs' PII does not, they face a separate issue. Plaintiffs do not allege that any portion of their credit unions' payments would go to data security. *See Perdue v. Hy-Vee, Inc*. 455 F. Supp. 3d 749, 766 (C.D. Ill. 2020) (dismissing unjust enrichment claim where "Plaintiffs have not alleged that any specific portion of their payments went toward data protection; rather, they state that their payments were for food and gas."). Faced with similar allegations against a restaurant, a Central District of Illinois Court dismissed the plaintiff's unjust enrichment claim because the plaintiff "paid for food products. She did not pay for a side order of data security and protection; it was merely incident to her food purchase." *Irwin v. Jimmy John's Franchise*, LLC, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016). Bearing in mind that "the court must draw on its judicial experience and common sense," *Iqbal*, 556 U.S. at 678-79, Plaintiffs paid for services from their credit unions which they presumably received, and their credit unions paid for software

from Bradford-Scott. Plaintiffs and their credit unions received those services or products with data security properly couched as incidental to such purchases. And without knowing what portion of those payments were allocated to data security, Plaintiffs' unjust enrichment claim is too speculative to survive dismissal.

The Court thus GRANTS Bradford-Scott's Motion to Dismiss as to Plaintiffs' unjust enrichment claim.

f. Bailment (Count VI)

Plaintiffs' final claim is for breach of bailment which Bradford-Scott contends must fail because it "never had exclusive control over Plaintiffs' information." (ECF No. 25-1 at 23). And indeed, a bailment claim requires full transfer of the property to the sole custody of the bailee such as to exclude the owner—or bailor—and all others. Relying on *Krupa*, 2023 WL 143140, Plaintiffs respond that it is a "reasonable inference" that Bradford-Scott did exclusively possess Plaintiffs' PII because, "once on Bradford-Scott's servers," Plaintiffs could not manipulate the information. (ECF No. 29 at 22). From Plaintiffs' perspective, Bradford-Scott was in full control of their PII. (*Id.*).

In Indiana, "[a] bailment arises when: (1) personal property belonging to a bailor is delivered into the exclusive possession of the bailee and (2) the property is accepted by the bailee." *Winters v. Pike*, 171 N.E.3d 690, 697 (Ind. Ct. App. 2021). "For delivery to occur, there must be a full transfer of the property, either actually or constructively, to the sole custody of the bailee such as to exclude the owner/bailor and others." *Id.* at 699. The Court agrees with Bradford-Scott that it is difficult to see how it was in "exclusive possession" of Plaintiffs' PII.

In *Krupa*—the primary case on which Plaintiffs rely—Judge Sweeney II held that the plaintiff, a data breach victim, "avoid[ed] the 'exclusive possession' problem" because "[Krupa]

was unable to manipulate his personal data on [the defendant's] servers; [the defendant] was in full control." 2023 WL 143140, at *10. No doubt *Krupa* supports the application of a bailment claim to this case. But since *Krupa* and under similar facts, Judge Magnus-Stinson held the opposite of Judge Sweeney II: "[I]n this case, Plaintiffs' PII was not in Defendants' exclusive possession. Plaintiffs were free to use or disseminate their PII as they pleased and deliver it to limitless others." *Johnson*, 2024 WL 2845928, at *8. This Court has gone on record as following the latter approach in the data breach context; that is, Plaintiffs' bailment claim must fail because Bradford-Scott was not in exclusive possession of Plaintiffs' PII. *See Mclaughlin, 2024 WL 4274848*, at *12 ("In line with Judge Magnus-Stinson, the Court declines to stretch the laws of bailment so far.").

While Plaintiffs' PII is property, the nature of the property leaves no avenue for Plaintiffs to argue that Bradford-Scott exclusively possessed it. Under Indiana law, delivery of the property to the bailee is essential to a bailment's creation and "sufficient delivery" requires "such a full transfer…as to exclude the owner and all other persons." *Stubbs v. Hook*, 467 N.E.2d 29, 31 (Ind. Ct. App. 1984). Plaintiffs here were not excluded from their PII. Even if Plaintiffs could not manipulate their PII once on Bradford-Scott's servers, Plaintiffs still had uninhibited access to their PII insofar as they could "deliver it to limitless others." *Johnson*, 2024 WL 2845928, at *8. Plaintiffs could use their PII to apply for mortgages, enroll for government benefits, and even sell it on the dark web if they wanted to. Moreover, Plaintiffs' credit unions also possessed their PII. The Court would be hard pressed to find exclusive possession where, as here, Plaintiffs' claim rests on the notion that some third-party must have also possessed their PII.

"*Krupa*…is an outlier case[,]" even among the Indiana district courts. *See Mclaughlin*, 2024 WL 4274848, at *12 (bailment claim dismissed for lack of exclusive possession) (J. Brady);

Johnson, 2024 WL 2845928, at *8 (same) (J. Magnus-Stinson); *Duffy v. Lewis Brothers Bakery* 2024 WL 5365032, at *15 (S.D. Ind. Dec. 19, 2024) (same) (J. Brookman). And the predominant view across the country is that bailment is not a viable theory "most often because the plaintiffs cannot plausibly allege that the defendant was in *exclusive* possession of their PII, simply given the nature of PII." *In re Numotion Data Incident Litig*., 2025 WL 57712, at *12 (M.D. Tenn. Jan. 9, 2025) (collecting cases).

The Court agrees with the weight of authority. Under no set of facts can Plaintiffs show that they were somehow excluded from possession of their own data. Indeed, Plaintiffs were and are free to do whatever they want with their PII. The Court simply cannot say Bradford-Scott exclusively possessed it. Lacking that essential element, Plaintiffs' bailment claim should be dismissed.

The Court thus GRANTS Bradford-Scott's Motion to Dismiss as to Plaintiffs' bailment claim.

g. Bradford-Scott's Motion to Strike

Lastly, Bradford-Scott moves to strike paragraphs 75 to 97 from Plaintiffs' Amended Complaint which it believes are impertinent and immaterial to this case. (ECF No. 25-1). Bradford-Scott argues that those paragraphs concerning "actions of identity thieves, statistics about cybercrime, and generic best practices for businesses…have nothing to do with the parties or facts of this case[.]" (*Id.* at 24). Plaintiffs respond that those allegations "give context to this litigation and are pertinent to the Court's understanding of the foreseeability of data security threats, the industry and regulatory standards by which [Bradford-Scott] is expected to abide, and the harm that consumers experience as a result of the compromise of PII." (ECF No. 29 at 23).

Under Rule 12(f), "[t]he court may strike from a pleading an insufficient defense or any

redundant, immaterial, impertinent, or scandalous matter." Fed. R. Civ. P. 12(f). "Rule 12(f) motions are disfavored and are ordinarily not granted unless the language in the pleading at issue has no possible relation to the controversy and is clearly prejudicial." *Mitchell v. Bendix Corp.*, 603 F. Supp. 920, 921 (N.D. Ind. 1985). And the Court must view the pleading at issue in the light most favorably to the pleader. *Lirtzman v. Spiegel*, 493 F. Supp. 1029, 1031 n.1 (N.D. Ill. 1980).

Although Bradford-Scott argues that the allegations at paragraphs 75 to 97 of the Amended Complaint are "designed to improperly inflame the issues[,]" it spilled little ink describing how. And the Court agrees with Plaintiffs that the allegations at issue do provide context for this litigation. The paragraphs concerning, as Bradford-Scott puts it, "actions of identity thieves" (ECF No. 20, ¶¶ 75-83) informs the worry and the potential harms that victims such as Plaintiffs face. The paragraphs concerning "statistics about cybercrimes" (*Id.* ¶¶ 84-87) are generally relevant to the foreseeability of the Incident. *See Doe v. Piraino,* 688 F. Supp. 3d 635, 667 (M.D. Tenn. 2023) ("The court finds the allegations regarding sexual misconduct involving non-entities in paragraphs 22 through 27 to be generally relevant to the question of whether the abuse at issue in this case was foreseeable. Although it is somewhat cumulative, it is not actually redundant or scandalous."). And the paragraphs concerning "generic best practices for businesses" (ECF No. 29, ¶¶ 88-97), which includes guidance from the FTC upon which Plaintiffs' negligence per se claim rests, informs the standard of care in this case. That said, the Court cannot say these allegations have "no possible relation to the controversy and [are] clearly prejudicial." *Mitchell*, 603 F. Supp. at 921. The Court therefore DENIES Bradford-Scott's Motion to Strike paragraphs 75 to 97 of Plaintiffs' Amended Complaint.

IV. Conclusion

For these reasons, Bradford-Scott's Motion to Dismiss (ECF No. 25) is DENIED as to Plaintiffs' claims for negligence and negligence per se; the motion is GRANTED as to all other claims; and Bradford-Scott's Motion to Strike is DENIED. Plaintiffs' claims for breach of implied contract, invasion of privacy, unjust enrichment, and bailment are DISMISSED.

SO ORDERED on February 20, 2025.

s/ *Holly A. Brady*
CHIEF JUDGE HOLLY A. BRADY
UNITED STATES DISTRICT COURT